REMARKS

Claims 1-11, 14, 16-27, and 37-57 are now pending in the application. Claims 12, 15, and 28-36 are cancelled. Claims 37-57 are added. Claims 1-6, 8, 10-11, 14, 16, 17, and 24 are amended. Support for the amendments and additions can be found throughout the originally filed application. Thus, no new matter is added. The Examiner is respectfully requested to reconsider and withdraw the rejection(s) in view of the amendments and remarks contained herein.

REJECTION UNDER 35 U.S.C. § 102

Claims 1-8, 10, and 13 stand rejected under 35 U.S.C. 102(b) as being anticipated by Birrell et al. (U.S. Patent 5,805,803). This rejection is respectfully traversed.

Birrell et al. disclose a method for a client 110 to access private resources 161, 162 and 163 that are located behind a firewall 130 and a tunnel 140. The method includes sending a communication request to the tunnel via an internetwork 120 and through the firewall; authenticating the request via a checker 141; and redirecting the communication to a proxy 143. The proxy then handles all communications between the private resources and the client.

However, Birrell et al. do not teach, "employing a distributed communication architecture, the architecture including: (a) at least one tunnel registration and look up service module supporting dynamic registration and access of communication data including one or more of the following types of information: (i) logical name; (ii) unique identifier; (iii) communication address; (iv) port; or (v) a service capability link pointing to a data type descriptor describing one or more of the following types of data: direct or

indirect tunneling; security information; tunnel protocol type; or address mapping information for distributed application modules; (b) at least one tunnel service software module that is independent from the existing security protection network devices to relay communication data for a local application module to an external network; (c) at least one tunnel session that is independent from the security network protection devices and can be dynamically configured to receive messages from and send messages to different ones of the application modules and a tunnel module co-located with a session control module; and (d) at least one tunnel message switching service supporting indirect tunneling specified in capability descriptors of tunnel sessions established between two or more remote tunnel services behind private networks; wherein employing the distributed communication architecture results in multiple application tunnel networks over multiple private networks that have the following properties: (a) without requiring design or configuration changes of the existing security protection network devices, the tunnel networks only require that one or more of the private networks allow for outgoing web access to one or more commonly accessible and secure web servers using a most common HTTP protocol; (b) the tunnel networks allow dynamic selection of additional tunneling methods based on allowable inbound and outbound filtering policies of the private networks; and (c) the tunnel networks only feed application communication module IP address, port number, and application data to tunnel service servers, thereby rendering a tunneling operation of an application independent and protected from administration of existing private networks" as recited in independent claim 1, especially as amended.

Accordingly, Applicants respectfully request the Examiner reconsider and withdraw the rejection of independent claim 1 under 35 U.S.C. § 102(b), along with rejection on these grounds of all claims dependent therefrom.

Claims 1, 12-23 and 36 stand rejected under 35 U.S.C. 102(b) as being anticipated by Nessett et al. (U.S. Patent 6,055,236). This rejection is respectfully traversed.

Nessett et al. disclose a distributed network address translation (DNAT) system and method for locating network services. The system includes computing devices on a LAN 12. A router 26 connects the LAN to a network access provider 34. Local IP addresses of the computing devices are not "globally unique" and therefore cannot be addressed by the network access provider. To work around this issue, the router maintains a table that correlates each of the local IP addresses to a group of port numbers. The groups of port numbers are all associated with a globally unique IP address that is assigned to the router. Third party devices, such as a telephone network 32 and an intranet or internet 30, can therefore communicate with the computing devices in the LAN by addressing them through their respective port numbers assigned to the router's globally unique internet address.

However, Nessett et al. do not teach, "employing a distributed communication architecture, the architecture including: (a) at least one tunnel registration and look up service module supporting dynamic registration and access of communication data including one or more of the following types of information: (i) logical name; (ii) unique identifier; (iii) communication address; (iv) port; or (v) a service capability link pointing to a data type descriptor describing one or more of the following types of data: direct or

indirect tunneling; security information; tunnel protocol type; or address mapping information for distributed application modules; (b) at least one tunnel service software module that is independent from the existing security protection network devices to relay communication data for a local application module to an external network; (c) at least one tunnel session that is independent from the security network protection devices and can be dynamically configured to receive messages from and send messages to different ones of the application modules and a tunnel module co-located with a session control module; and (d) at least one tunnel message switching service supporting indirect tunneling specified in capability descriptors of tunnel sessions established between two or more remote tunnel services behind private networks; wherein employing the distributed communication architecture results in multiple application tunnel networks over multiple private networks that have the following properties: (a) without requiring design or configuration changes of the existing security protection network devices, the tunnel networks only require that one or more of the private networks allow for outgoing web access to one or more commonly accessible and secure web servers using a most common HTTP protocol; (b) the tunnel networks allow dynamic selection of additional tunneling methods based on allowable inbound and outbound filtering policies of the private networks; and (c) the tunnel networks only feed application communication module IP address, port number, and application data to tunnel service servers, thereby rendering a tunneling operation of an application independent and protected from administration of existing private networks" as recited in independent claim 1, especially as amended. Nor do Nessett et al. teach that "said look-up service does not limit a number of entries for each communication session

between two tunnel services, thereby allowing applications to group multiple message queues to create parallel communication channels between a pair of tunnel services" as recited in independent claim 16, especially as amended.

Accordingly, Applicants respectfully request the Examiner reconsider and withdraw the rejection of independent claims 1 and 16 under 35 U.S.C. § 102(b), along with rejection on these grounds of all claims dependent therefrom.

REJECTIONS UNDER 35 U.S.C. § 103

Claims 9, 11, 24-33 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett et al. (U.S. Patent 6,055,236) in view of Birrell et al. (U.S. Patent 5,805,803). Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett and Birrell in view of Mei. Applicants respectfully traverse these rejections.

For discussion of the differences between Applicants' claimed invention and the teachings of Nessett et al. and Birell et al., Applicants respectfully direct the Examiner's attention to remarks detailed above with respect to rejection under 35 U.S.C. § 102(b). Applicants further assert that Mei does not teach these differences. Applicant's still further assert that the combined teachings of Nessett et al. and Birell et al. and Mei do not teach teach, suggest, or motivate these differences. These differences are significant.

Accordingly, Applicants respectfully request the Examiner reconsider and withdraw the rejection of independent claims 1 and 16 under 35 U.S.C. § 103(a), along with rejection on these grounds of all claims dependent therefrom.

CONCLUSION

It is believed that all of the stated grounds of rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider and withdraw all presently outstanding rejections. It is believed that a full and complete response has been made to the outstanding Office Action, and as such, the present application is in condition for allowance. Thus, prompt and favorable consideration of this amendment is respectfully requested. If the Examiner believes that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at (248) 641-1600.

Respectfully submitted,

Dated: January 18, 2006

By: _____
Jennifer S. Brooks
Reg. No. 51,501

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. Box 828
Bloomfield Hills, Michigan 48303
(248) 641-1600

GAS/JSB